



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/865,246	05/25/2001	Morton Gregory Swimmer	YOR920010310US1	3963
54105	7590	08/22/2006	EXAMINER ZAND, KAMBIZ	
DUKE W. YEE YEE & ASSOCIATES, P.C. P.O. BOX 802333 DALLAS, TX 75380			ART UNIT 2132	PAPER NUMBER

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/865,246

Applicant(s)

SWIMMER ET AL.

Examiner

Kambiz Zand

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 June 2006.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-67 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☒ Claim(s) 1-12, 24, 26-37 and 47-58 is/are allowed.
6) ☒ Claim(s) 13-23, 25, 38-46 and 59-67 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 05/21/2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 4-5, 7, 12-13, 20, 22, 24-26, 29, 30, 32, 37, 38, 45, 47, 50, 51, 53, 58, 59 and 67 have been amended.
4. Claims 1-67 are pending.

Response to Applicant's Arguments

5. Applicant's arguments with respect to the claims have been considered and they are persuasive with respect to claims 1-12, 24, 26-37, 47-58. the rejections of claims 1-12, 24, 26-37 and 47-58 have been withdrawn.
6. Applicant's arguments with respect to other claims are not persuasive since the concepts of the arguments are not present in the claim language in the manner similar to claim 1 (which is clear), and therefore the rejections are maintained. The added limitations do not add any clarity in that manner and just repeat what already is inherent in the claims limitations.

Claim Rejections - 35 USC § 102

7. **Claims 13-20, 22-23, 25, 38-45, and 59-66** are rejected under 35 U.S.C. 102(b) as being anticipated by Dotan (5,822,517 A).

Applicant has described journaling on page 3 lines 8-9 of the specification in the "summary of the invention" as follows: "journaling involves storing a system state before an action is executed so that the state can be restored upon demand".

Applicant further described "the detection of the virus may be performed by using pattern matching on system audit trail in which system audit contain activities occurring within the data processing system" on the same page lines 9-11.

Furthermore applicant described "journaled data" being used for the following reasons: "in response to an identification of the virus, the data is restored to its previous state using the journaled data" see page 3, lines 11-13.

Therefore based on the above definition by applicant the following new ground of rejection has been rendered.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

As per claims 13, 38 and 59 Dotan (5,822,517 A) teach a data processing system, a computer program product in a computer readable medium, a method in a data

processing system for repairing damage to data (see fig.3 & 4 and associated text where Dotan disclose method steps of 54 and 64-66 for protecting a program, restoring to initial state which corresponds to applicant's "repairing the damaged data in relationship with data processing system of fig.1 and associated text which corresponds to applicant's limitation "data processing system"), the method, means and instructions comprising: saving a state of a data object in response to a request to access the data object by a process (see step 54 of fig.3 and 4 where the action of memorizing current program state as "initial program state" corresponds to Applicant's limitation "saving a state of data object" that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state; and step 52 of fig.4 and associated text corresponds to applicant's limitation "request to access"; also see col.4, lines 27-30), method, means and instructions for performing pattern matching of a set of actions taken within the data processing system (see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation "performing pattern matching of set of actions"; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps) and method, means and instructions for determining whether an unauthorized intrusion has occurred in response to performing pattern matching and if so (see step 64 of fig.4 and associated text where generating alarm corresponds to Applicant's "responsive to an identification of the virus"; also see col.7, lines 20-26) ,

method, means and instructions for initiation a rollback to return the data object back to its saved state (**see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant "rollback ...to its saved state"**).

As per claim 22 Dotan (5,822,517 A) teach an intrusion protection system for use in a data processing system (**see abstract; fig.1 and associated text; col.3, lines 44-67; col.4, lines 1-11 which disclose an intrusion detection system**) comprising: a sensor filter, wherein the sensor filter receives requests to access data within the data processing system from a process (**step 52 of fig.4 and associated text corresponds to applicant's above limitation; see col.6, lines 14-18; also see col.4, lines 27-30**); a pattern matcher, wherein the pattern matcher receives actions initiated by the process, compares the actions to a pattern to form a comparison, determines whether an unauthorized intrusion has occurred (**see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant's limitation determining whether an unauthorized intrusion present; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps is a virus detection determination step**), generates a first indication in response to an identification of an absence of an unauthorized intrusion (**see step 62 of fig.4 and associated text where a matching disclose Applicant's above limitation; also see col.7, lines 20-26**), and generates a second indication to restore the data to a

prior state in response to an identification of the unauthorized intrusion (**see step 64 and 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant journaled data**); and a journaler, wherein the journaler journals data in response to accessing of the data and restores the data to the prior state in response to the indication by the pattern matcher, wherein the data is journaled until the first indication is generated by the pattern matcher (**see step 68 and associated text; col.7, lines 37-51 where it disclose restoring the program using the stored program's initial state which corresponds to applicant journaled data**).

As per claim 25 Dotan (5,822,517 A) teach a data processing system (see fig.1 and associated text which corresponds to applicant's data processing system) comprising: a bus system; a communications unit connected to the bus system; a memory connected to the bus system (see col.5, lines 57-67; col.6, lines 1-9 where it disclose the data processing system; communication unit, a bus system and connection between different devices through bus system is inherent features of a data processing system (please see any computer architecture books for meaning of the bus system and its relationship with other data system processing modules including the cpu), it is inherent where the cpu, memory I/O modules, controllers and other devices are communicate through bus system), wherein the memory includes a set of instructions (see col.6, lines 1-12); and a processing unit connected to the bus system (inherent part of

the data processing system), wherein the processing unit executes the set of instructions to save a state of a data object in response to a request to access the data object by a process (see step 54 of fig.3 and 4 where the action of memorizing current program state as “initial program state” corresponds to Applicant’s above limitation that is storing the initial state of the data; see col.4, lines 27-35 where it disclose the act of storing the initial state of the program); perform pattern matching of a set of actions taken within the data processing system (see step 60 of fig.3 and 4 and associated texts where the act of determination of the matching between initial state and the final state corresponds to applicant’s limitation “performing pattern matching of set of actions”; also see col.4, lines 20-28; col.7, lines 20-26 where it disclose the matching method steps); and determine whether an unauthorized intrusion has occurred in response to performing pattern matching (see step 60, 64 associated text; col.7, lines 37-51 where it disclose determination, unauthorized intrusion has occurred which corresponds to applicant above limitation).

As per claims 14, 39 and 60 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the performing step comprises: comparing the set of actions to a pattern from a set of patterns to form a comparison; determining whether the comparison indicates that the unauthorized intrusion has occurred; and responsive to an absence of the unauthorized intrusion, repeating the comparing

step using another pattern from the set of patterns **(see as applied to the independent claims above with respect to steps 52-66; col.6 which disclose this action is a continuation process for an invocation of access request).**

As per claims 15, 40 and 61 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the performing step comprises: matching patterns with the set of actions; determining whether the unauthorized intrusion has occurred; if an intrusion is absent, determining whether a time threshold has been reached; and if an absence of a reaching of the time threshold is present, repeating the matching step using another set of actions **(see as applied to the independent claims above with respect to steps 52-66; col.6 which disclose this action is a continuation process for an invocation of access request; and the step 64 generating the alarm corresponds to applicant's threshold limitation).**

As per claims 16, 41 and 62 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions identifies an absence of the unauthorized intrusion **(see step 62 of fig.4 and associated text where a matching disclose Applicant's above limitation; also see col.7, lines 20-26).**

As per claims 17, 42 and 63 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion (**see step 60 and 64 of fig.4 and associated text; col.7**).

As per claims 18, 43 and 64 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by a virus (**see col.7, lines 52-66**).

As per claims 19, 44 and 65 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by an authorized user input (**see col.6, lines 1-4**).

As per claims 20, 45 and 66 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59 further comprising: saving a state of all data objects within the data processing system (**see step 54 of fig.4 and associated text; see col.6-7**).

As per claim 23 Dotan (5,822,517 A) teach all limitation of the claims but do not disclose, wherein the intrusion protection system is located within an operating system (**see col.6, lines 8-13**).

Claim Rejections - 35 USC § 103

8. **Claims 21,46, and 67** are rejected under 35 U.S.C. 103(a) as being unpatentable over Dotan (5,822,517 A) in view of Conklin et al (5,991,881 A).

As per claims 21, 46, and 67 Dotan (5,822,517 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26, 13, 38, 59 and 47 as applied to claim 1 above but do not explicitly disclose, wherein the data is located in a storage device external to the data processing system. However Conklin et al (5,991,881 A) disclose wherein the data is located in a storage device external to the data processing system (**see fig.3, 4 and associated text where the storage within the hosts are external to monitoring system**). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Conklin's storage external device in Dotan's software detection system in order to have no discernible address and can not be accessed by an intruder or hacker (see col.1, lines 66-67; col.2, lines 1-2).

Allowable Subject Matter

9. Claims 1-12, 24, 26-37 and 47-58 are allowed.

Conclusion


10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as

Art Unit: 2132

(571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


KAMBIZ ZAND
PRIMARY EXAMINER

08/17/2006

AU 2132